P24

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/386,341	08/31/1999	RYU INADA	104116	1319

25944 7590 08/13/2003

OLIFF & BERRIDGE, PLC
P.O. BOX 19928
ALEXANDRIA, VA 22320

EXAMINER
NOBAHAR, ABDULHAKIM

ART UNIT	PAPER NUMBER
2132	5

DATE MAILED: 08/13/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/386,341	Applicant(s) INADA, RYU	
	Examiner Abdulhakim Nobahar	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____ .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-19 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-19 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 8/31/99 is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and, *In re Thorington,* 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 1-6 and 8-19 are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-23 of U.S. Patent No. 6,530,020. Although the conflicting claims are not identical, they are not patentably distinct from each other because the claims of the application are a broader recitation of the patented claims. The claims in the examined application do not expressly specify the generation of a group having one or more members M_i (i=1 to n) and the public and secret keys (P_{Mi} and S_{Mi}) of the members. Because the claims in the application are broader and they are further rejected over the prior art cited below.

With regard to pending claims 1-3, 5 and 14-15, the claims 1-2, 4-7 and 14 of the patent anticipate the generation (corresponds to the recited acquiring in the pending claims) of public and secret (private) keys for both group and the members of the group in a readable recording medium and the group keys are allocated to the group. The secret key of the group is encrypted by each of the members' public key and decrypted by the respective members' secret keys. A combination of public key, encrypted secret keys, public and private keys of a member are arranged in a composite lock. A cryptogram information which is an encryption/decryption key is encrypted and decrypted by use of the public and the corresponding secret (private) keys included in the composite lock. Although the conflicting claims are not identical, they are not patentably distinct from each other because the abovementioned pending claims are generic to the method recited in the abovementioned patent's claims. The recitation of allocation process in claim 1 of the patent, the arrangement process of keys in claim 4 of the patent and the replacement operation of keys in claim 7 of the patent which all happen in a readable recording medium indicate that the composite lock (corresponding to the recited lock data in pending claims) are stored in each group unit. And the cryptogram information in the patent corresponds to the recited target data in the pending claims. Since the recited secret key of the group in the patent shared by all members of the group, thus it is a species of the generic category defined by the common key of the pending claims.

With regard to the pending claim 4 that contains the element of writing a signature in addition to the storing lock data and decrypting common and private keys included in the pending claim 1, the claims 8-9 and 17-18 of the patent recites the execution or performing (corresponding to the recited writing in the pending claim 4) of an electronic signature using the secret (private) key included in the composite lock that has been produced by using the public key corresponding to the said secret key. Specifically claims 9 and 18-19 of the patent recite that the electronic signature is obtained (acquired) by using the secret key with respect to the data containing the produced keys. Although the conflicting claims are not identical, they are not patentably distinct from each other because with respect to writing a signature the pending claim 4 is identical in scope compared to the claims 8-9 and 17-18 of the patent. The other elements of the pending claim 4 are identical to respective elements in the pending claim 1 which in turn are anticipated by the elements of claim 1 of the patent as stated above.

With regard to pending claim 6, the claims 6 and 17-19 of the patent recite the replacement of the public and secret (private) keys that are changed in response to the change in the structure of the composite lock. The changing of the secret key could happen by any process such as using an inverse function as recited in the pending claim. One having ordinary skill in the art would have been motivated to make such a modification to the secret key because that embodiment is disclosed as being a preferred embodiment within the claim 17

and 18 of the patent. The same that was applied to the elements of the pending claim 1 above is applied to the like elements of the pending claim 4.

With regard to pending claim 8, the claims 17-18 of the patent recites the performing of an electronic signature by using the secret (private) key of a composite lock which includes the encrypted said secret key and the corresponding public key belonging to a member authorized to implement changes (changing right holder) that is used in the verification process of a signature. Although the conflicting claims are not identical, they are not patentably distinct from each other because with respect to writing and verifying a signature the pending claim 8 is identical in scope compared to the claims 17 of the patent.

With regard to pending claim 9, the same is applied as stated for the like elements of the pending claims 1, 4 and 8 above.

With regard to pending claim 10, the same is applied as stated for the like elements of the pending claim 4 above and further the claims 7-9 and 17 of the patent recites the replacement of the public and private keys in the composite lock by a new pair of keys for the changing right owner (holder) that are used for signing (writing) an electronic signature. Although the wording of the conflicting claims are different, they are not patentably distinct from each other because with respect to changing the keys in a composite lock for a changing right holder and

writing a signature the pending claim 8 is identical in scope compared to the claims 7-9 and 17 of the patent.

With regard to pending claim 11, the claim 10 of the patent recites that the composite lock (corresponding to the recited lock data in the pending claim) owns a version discriminator (identifier), which indicates the version number of the composite lock. Although the wording of the conflicting claims is different, they are not patentably distinct from each other because the pending claim is identical in scope compared to the claim 10 of the patent.

With regard to pending claim 12, the claim 11 of the patent recites that the composite lock owns a preceding version handling discriminator that corresponds to the recited precedent version dealing in the pending claim and defines (control) the handling of the composite data. Although the wording of the conflicting claims is different, they are not patentably distinct from each other because the pending claim is identical in scope compared to the claim 10 of the patent.

With regard to pending claim 13, the claim 13 of the patent recites that the preceding version handling discriminator contains information for discriminating as to whether or not said composite lock has been changed and claim 11 of the patent recites that the version handling discriminator is to define handling of a

just-before-set version of said composite lock that is identical in scope with the pending claim 13. Therefore, while the wording of the conflicting claims is different, they are not patentably distinct from each other.

With regard to pending claim 16, the same is applied as stated for the like elements of the pending claims 1-3 and 5 above.

With regard to pending claim 17-19, the same are applied as stated for the like elements of the pending claims 1-5 and 9 above.

Specification

1. The lengthy specification has not been checked to the extent necessary to determine the presence of all possible minor errors. Applicant's cooperation is requested in correcting any errors of which applicant may become aware in the specification.

2. A substitute specification in proper idiomatic English and in compliance with 37 CFR 1.52(a) and (b) is required. The substitute specification filed must be accompanied by a statement that it contains no new matter.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any

person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

1. Claim 7 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter, which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

2. Claim 7 contains "redundant data generating function" and "to generate redundant data", which are not specified or explained in the specification of the claimed invention.

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claims 1, 3-4 and 7 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

4. Claim 1 in line 7, contains "group/member". There is insufficient antecedent basis for this in the claim.

5. Claims 3 and 4 in lines 8-13 states "a step for decrypting one of said encrypted common keys included in said lock data by use of the private key corresponding to said group/member to generate said common key; and

a step for decrypting said encrypted private key included in said lock data by use of said decrypted common key to generate said private key."

It is unclear that whether the private key is used to decrypt the encrypted common key is the same private key, which is encrypted and being decrypted by the decrypted common key or different. Why it is needed to decrypt the said encrypted private key by use of said decrypted common key to generate the said private key, If that private key (corresponding to the public key used for encryption of common key) is already provided?

6. Claim 4 in line 14, recites the limitation "signature target data". There is insufficient antecedent basis for this limitation in the claim.

7. Claim 7 in line 7, recites the limitation "redundant data generating function". There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

Claims 1-6 and 8-19 are rejected under 35 U.S.C. 102(e) as being anticipated by US Patent 6,530,020 B1 issued to Aoki.

The applied reference has a common assignee with the instant application. Based upon the earlier effective U.S. filing date of the reference, it constitutes prior art under 35 U.S.C. 102(e). This rejection under 35 U.S.C. 102(e) might be overcome either by a showing under 37 CFR 1.132 that any invention disclosed but not claimed in the reference was derived from the inventor of this application and is thus not the invention "by another," or by an appropriate showing under 37 CFR 1.131.

Regarding claims 1-4 and 14-15, Aoki discloses:

A step for storing lock data which includes a public key, an encrypted private key formed by encrypting a private key corresponding to said public key by use of a common key, and a plurality of encrypted common keys generated by encrypting said common key by use of respective public keys of the group/members. See, for example, column 8, line 17-column 9, line 23 and column 10, lines 5-12.

A step for encrypting encryption target data by use of the public key of said lock data. See, for example, column 3, lines 12-19.

The method for encryption as claimed in claim 1, wherein said encryption target data is a decrypting key used for decrypting encrypted information. See, for example, column 2, line 61-column 3, line 19.

A step for decrypting one of said encrypted common keys included in said lock data by use of the private key corresponding to said group/member to generate said common key. See, for example, column 3, lines 5-11 where the group secret key corresponds to the recited common key and member secret key corresponds to the recited private key and column 18, lines 1-8.

A step for decrypting said encrypted private key included in said lock data by use of said decrypted common key to generate said private key. See, for example, column 23, line 59-column 24, line 3. Although this step is redundant because already the private key is available and unencrypted, examiner assumes that the decrypted common key is to decrypt an encrypted plain text.

A step for acquiring encryption target data encrypted by use of said public key. See, for example, column 3, lines 5-19 where the cryptogram corresponds to the recited target data.

A step for decrypting said encrypted encryption target data by use of said decrypted private key. See, for example, column 3, lines 5-19 where the group secret key corresponds to the recited private key.

A step for storing and acquiring signature target data on which a signature to be verified by use of said public key is to be written; and a step for writing a signature on said signature target data by use of said decrypted private key. See, for example, column 2, lines 56-60, column 4, lines 42-46 and Fig. 15.

Referring to claim 5, this claim is rejected as applied to like elements of claims 1-4 above, and further Aoki discloses:

A step for acquiring a pair of a public key and a private key. See, for example, column 10, lines 1-5 and column 12, lines 16-25.

A step for acquiring a common key. See, for example, column 21, lines 16-20.

Referring to claim 6, this claim is rejected as applied to like elements of claims 1-5 above, and further Aoki discloses:

A step for modifying the private key by use of a desired function including an inverse function to generate a modified private key. See, for example, column

4, lines 33-46 where changing secret key corresponds to the recited modifying the private key.

Regarding claim 8, Aoki discloses:

The lock data further includes a public key for verifying a signature, an encrypted signature private key which is formed by encrypting a signature private key for writing said signature by use of a public key of a changing right holder, and a signature written by use of said signature private key on desired data included in said lock data. See, for example, column 1, lines 47-50, column 4, lines 42-46 and column 18, lines 13-35.

Referring to claim 9, this claim is rejected as applied to like elements of claims 1-5 above, and further Aoki discloses:

a second public key for verifying a signature, an encrypted signature private key formed by encrypting a signature private key for writing said signature by use of a public key of a changing right holder, said first public key, said encrypted private key, said encrypted common key, said second public key, and a signature written by use of said signature private key on said encrypted signature private key. See, for example, column 9, lines 14-23, column 13, lines 36-47, column 13, lines 54-60 and column 14, lines 17-25.

a step for decrypting said encrypted signature private key included in said lock data by use of said private key of a changing right holder; a step for changing said lock data; and a step for writing a signature on the changed lock

data by use of said signature private key. See, for example, column 4, lines 36-47, column 8, line 54- column 9, line 12 and column 14, lines 4-20.

Regarding claim 10, Aoki discloses:

a step for changing said second public key;

a step for changing said signature private key;

a step for changing said encrypted signature private key before changing by use of a new encrypted signature private key newly formed by encrypting a changed signature private key by use of said public key of a changing right holder; and

a step for writing a signature by use of said signature private key after changing. See, for example, column 4, line 47-column 5, line 29.

Regarding claim 11, Aoki discloses:

The method for changing lock data as claimed in claim 9, wherein said lock data has a version identifier that indicates the version of said lock data. See, for example, column 8, lines 60- column 9, line 12.

Regarding claims 12-13, Aoki discloses:

The method for changing lock data as claimed in claim 9, wherein said lock data has a precedent version dealing identifier, and controls how to deal with the lock data of the precedent version based on the identifier; and said precedent version dealing identifier includes the information that identifies whether the

change of said lock data should be applied retroactively or not. See, for example, column 7, lines 47-61, column 8, line 60-column 9, line 12 and column 14, lines 40-56 where value indicative of handling of just-before-set version corresponds to the recited version dealing idetifier.

Referring to claim 16, this claim is rejected as applied to like elements of claims 1-5 above, and further Aoki discloses:

a generation part that decrypts one of said encrypted common keys included in said lock data by use of said private key corresponding to a group/member; and a generation part that decrypts said encrypted private key included in said lock data by use of said decrypted common key to generate said private key; an acquiring part that acquires encryption target data encrypted by use of said public key; and a decrypting part that decrypts said encrypted encryption target data by used of said decrypted private key. See, for example, column 3, lines 20-50.

Referring to claims 17-18, these claims are rejected as applied to like elements of claims 1-5 and 16 above.

Referring to claim 19, this claim is rejected as applied to like elements of claims 1-5, 9 and 16 above.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Aoki (6,530,020) in view of Gressel et al (5,852,665) (hereinafter Gressel).

Referring to claim 7, Aoki discloses:

a step for acquiring a pair of a public key and a private key. See, for example, column 10, lines 1-5 and column 12, lines 16-25.

a step for acquiring a common key. See, for example, column 21, lines 16-20.

a step for encrypting said private key by use of said common key to generate an encrypted private key; and a step for combining said public keys, said encrypted private key, and said encrypted common keys to generate lock data. See, for example, column 8, line 17-column 9, line 23 and column 10, lines 5-12.

However, Aoki does not expressly disclose:

a step for executing redundant data generating function on respective public keys of group/members to generate redundant data; a step for encrypting a combination of said common key and said redundant data by use of said

respective public keys of group/members to generate corresponding encrypted common keys.

Gressel teaches a method for cryptographic communications among entities that concatenates the secret session key with a random numbers and uses a public key to encrypt the combination. The random number is the result of a XOR operation that corresponds to the recited redundant data generating function execution. See, for example, column 10, lines 59-66 and column 11, lines 24-41.

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the encrypted concatenation of the session (common) key as taught in Gressel in the system of Aoki, because it would provide a controlled balance for ensuring confidentiality for the people communications while allowing legitimate law enforcement agencies the ability to make controlled responsible interception of messages sent by suspect individuals and organizations. See column 2 lines 51-56.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

US Patent No. 5,748,736 to Mittra teaches a method for secure group communication via multicast or broadcast transmission of encryption keys and data.

US Patent No. 5,867,578 to Brickell et al teaches a method for a multi-step digital signature in a group communication.

US Patent No. 5,953,419 to Lohstroh et al teaches a system for distributing secured versions of a file decryption key to members of a group.

US Patent No. 6,052,469 to Johnson et al teaches a system for handling key recovery and permitting users to establish a session key.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Abdulhakim Nobahar whose telephone number is 703-305-8074. The examiner can normally be reached on M-F 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 703-305-1830. The fax phone numbers for the organization where this application or proceeding is assigned are 703-746-7239 for regular communications and 703-746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Abdulhakim Nobahar
Examiner
Art Unit 2132

AN
August 10, 2003

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100